Release Notes

McAfee Endpoint Encryption for PC 7.0.3

Contents

- *About this release*
- *Resolved issues*
- *Installation instructions*
- *Known issues*
- *Additional information*
- *Find product documentation*

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

Important

We do not support the automatic upgrade of a pre-release software version. To upgrade to a production release of the software, you must first uninstall the existing version.

Release build – 7.0.3.413

This release was developed for use with:

- McAfee® ePolicy Orchestrator 4.6.4, 4.6.5, 4.6.6, 4.6.7
- McAfee® ePolicy Orchestrator 5.0.1

Note

Note this release supports upgrading to McAfee Drive Encryption 7.1, see PD24867 Drive Encryption 7.1 Product Guide page 31 for more details.

Purpose

This release of McAfee® Endpoint Encryption for PC (McAfee EEPC) fixes issues that were reported in the previous versions.

Rating

High Priority – McAfee considers this release to be high priority for supported Windows versions. Failure to apply a high Priority update may result in potential business impact.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release. This release includes all the fixes from previous releases.

- When using a Fujitsu Esprimo Mobil v6515 or v6555, the preboot authentication screen is not shown. This issue is now addressed; the systems have been added to the list of machines that do not support IRQ handlers. (Reference: 897095)
- In some systems the message "Waiting for information" appears and the activation never starts; this was caused by issues during architecture detection (BIOS or UEFI). This issue is now addressed; and the product is now able to determine the platform architecture. (Reference: 910647, 909993)

- When using an HP Compaq 8100 Elite system with Smartcard Tokens being read from an external USB card reader, the preboot authentication freezes. This is now addressed by adding this system to the list of systems that do not support USB hand back to the BIOS. (Reference: 912406)
- When using a Panasonic CF-AX2 system some key presses on the built-in keyboard at preboot cause the system to freeze. This issue is now addressed and the key presses no longer cause the system to hang. (Reference: 906171)
- When using a Dell XPS 13 system, the built-in keyboard and mouse pad fail to work after a warm reboot. This issue is now resolved and the preboot is handling the keyboard and mouse pad correctly after a warm reboot. (Reference: 893568)
- When upgrading the EEPC extensions from a previous version, the extension check-in may fail or take a substantial amount of time to complete the check in. This is now addressed and the extension check-in completes correctly. (Reference: 918082)
- On some systems when a removable device is attached, a popup in Windows will appear stating that the device is formatted. This is caused by 3rd party drivers reacting to the EEPC driver responses. This is now addressed and the EEPC driver is exempted from interacting with those devices. (Reference: 916774, 910623)
- On a system containing two hard drives, if the secondary drive is a GPT disk, the second drive is not encrypted. This is now addressed and the second drive is encrypted correctly. (Reference: 911379)
- When upgrading from a previous Endpoint Encryption for PC version, if the system is unattended the upgrade fails. This is now addressed and the upgrade will run on unattended systems. (Reference: 934324)
- After upgrading from a previous Endpoint Encryption for PC version, the new feature to display the CAPS LOCK icon when CAPS LOCK is on may not display. This is now addressed; after upgrade the CAPS LOCK icon is correctly shown. For more information please refer to KB80062. (Reference: 935267)
- On a Dell Latitude E5430 system running in UEFI mode, when the shift keys are pressed the characters are randomly replaced with erroneous characters. This issue is now addressed and the preboot UEFI environment is able to handle this system correctly. (Reference: 928864)

Installation instructions

For information about installing or upgrading McAfee Endpoint Encryption for PC, see *Product Guide McAfee Endpoint Drive Encryption 7.0 Patch 1* - PD24423.

Requirements

Make sure that your system meets these requirements before installing the software.

Systems	Requirements
McAfee ePolicy Orchestrator (ePO) server systems	• See the product documentation for your version of McAfee ePO. **Important** This release of EEPC does not support ePO 5.1.
McAfee Agent	• McAfee Agent for Windows 4.6 and later versions. ○ Note Windows 8 support requires McAfee Agent 4.6.1 or above.

Systems	Requirements
Client systems for EEPC	• **CPU**: Pentium III 1GHz or higher • **RAM**: 1 GB minimum (2 GB recommended) • **Hard Disk**: 200 MB minimum free disk space ○ For more requirements on Intel® AMT Systems see the product documentation for ePO Deep Command product.

Software requirements

Software	Requirements
McAfee management software	McAfee® ePolicy Orchestrator 4.6.4, 4.6.5, 4.6.6, 4.6.7 McAfee® ePolicy Orchestrator 5.0.1 For the latest information regarding supported environments please consult Supported Environments for Endpoint Encryption for PC 7.x on Microsoft Windows KB76804.

Operating system requirements

Systems	Software
Client systems	• Windows Server 2008 (32- and 64-bit) • Windows XP SP3 (32-bit only) • Windows Vista SP2 (32- and 64-bit) • Windows 7 and SP1 (32- and 64-bit), (Not XP Mode) **Note** For Opal activation, Windows 7 SP1 is required. • Windows 8 (32- and 64-bit) **Note** EEPC 7.x supports Windows 8 in UEFI boot mode only on Windows 8 logo certified hardware. For the latest information regarding supported environments please consult Supported Environments for Endpoint Encryption for PC 7.x on Microsoft Windows KB76804.

Known issues

For a list of known issues in this product release, refer to McAfee KnowledgeBase article KB79501.

Additional information

Product documentation

This release of EEPC 7.0 Patch 3 includes the following documentation set.

Standard product documentation

McAfee documentation provides the information you need during each phase of product implementation, from installing a new product to maintaining existing ones. This release of EEPC 7.0 Patch 3 includes the following documents:

- McAfee Endpoint Encryption for PC 7.0 Patch 3 Release Notes (this document)

Knowledgebase articles

- McAfee Endpoint Encryption for PC 7.x (FAQ): KB76591
- McAfee Endpoint Encryption for PC version 6.x and 7.x error messages: KB67358
- McAfee Endpoint Encryption for PC 7.x – Supported Environments: KB76804
- Read this before installing EEPC: KB68411
- Opal-based disk drive support: KB75045
- Accessing Windows Safe Mode when Endpoint Encryption for PC 6.x/7.x is installed: KB73714
- How do the recovery tools for Windows 8 interact with EEPC: KB76638

Note Windows Recovery Console (F8 recovery) is not available on Samsung Slate 700T tablets because technical issues prevent F8 recovery from working on this platform in EEPC 7.x.

Note For general information about the recovery tools available with McAfee EEPC 7.x please refer to the McAfee Endpoint Encryption for PC 7.x (FAQ) KB76591

- Tablet Support for Endpoint Encryption for PC 6.2 Patch 1 and later: KB78049

Supported tokens and readers

McAfee Endpoint Encryption for PC supports different logon tokens and token readers. The token type associated with a user or a group can be modified using McAfee ePO. For details on modifying tokens, see the *McAfee Endpoint Drive Encryption 7.0 Patch 1 Product Guide.*

KnowledgeBase articles for tokens and readers in EEPC 7.x

For more information about supported tokens and readers, refer to these KnowledgeBase articles:

- Supported Tokens used for authentication in McAfee Endpoint Encryption for PC 7.x KB76589
- Supported Readers used for authentication in McAfee Endpoint Encryption for PC 7.x KB76590

Support for self-encrypting Opal-based disk drive

EEPC 7.0 Patch 3 provides support for self-encrypting Opal-based disk drives on UEFI and BIOS.

UEFI

Opal-based self-encrypting disk drives will be supported on UEFI systems where the system is Windows 8 logo compliant and if the system was shipped from the manufacturer fitted with an Opal self-encrypting drive.

Opal-based self-encrypting disk drives might not be supported on UEFI systems if the system is not Windows 8 logo compliant, or if the system did not ship from the manufacturer fitted with an Opal self-encrypting drive.

This is because a UEFI security protocol that is required for Opal management is only mandatory on Windows 8 logo compliant systems where an Opal-based self-encrypting disk drive is fitted at the time of shipping. Those shipped without self-encrypting drives might or might not include the security protocol. Without the security protocol, Opal management is not possible.

Note EEPC 7.0 Patch 3 will support the Opal-based encryption provider on UEFI systems fitted with an Opal-based disk drive if the UEFI protocol **EFI_STORAGE_SECURITY_COMMAND_PROTOCOL** is present on the system.

BIOS

Opal is supported for Opal-based disk drives under BIOS. To activate a system using the native Opal functionality, Windows 7 SP1 Operating system and above is required. On systems with Opal-based disk drives where the Operating System is Windows 7 RTW or below, PC software encryption will be used.

Note By default, software encryption will be used on both Opal and non-Opal based systems in EEPC 7.0 Patch 3.

To make sure that Opal technology is chosen in preference to software encryption, we recommend you always set Opal as the default encryption provider by moving it to the top of the list on the Encryption Providers page. This makes sure that Opal locking is used on Opal-based disk drives. For more information about Opal, refer to the FAQs available in KB76591.

Reimaging Opal drives

When an Opal system (activated using the Opal encryption provider) is reimaged and restarted without first removing Endpoint Encryption, the user is locked out of the system. This happens because:

- The Pre-Boot is held off the disk and it is still active when the system is restarted.
- The Pre-Boot File System is destroyed during the imaging process.

Note On BIOS systems, IDE and RAID modes are not supported with Opal. For more information regarding Opal support, please review the KnowledgeBase article KB75045. Opal activation might occasionally fail because the Microsoft defragmentation API used fails to defragment the host. For this to happen, the activation will restart at the next Agent-Server Communication Interval (ASCI).

Before installing EEPC 7.0 Patch 3

Make sure that you read this section completely and take the following precautions before installing EEPC 7.0 Patch 3 on the client. For more information on the user experience when upgrading from EEPC 7.0 Patch 3 to McAfee Drive Encryption 7.1 please consult PD24867 Drive Encryption 7.1 Product Guide page 31 for more details.

Support for upgrade to McAfee Drive Encryption 7.1

This release supports upgrading to McAfee Drive Encryption 7.1.

Hardware Disk hardware failure during Encryption

We recommend running a CHKDSK /r prior to installing EEPC to make sure the hard disk is in a healthy state. If the Hard Disk is damaged or has a high number of undiscovered bad sectors, the disk could fail during the full disk encryption process.

In addition, we recommend using Endpoint Encryption GO to discover potential issues prior to installation. For more information, see KB72777.

Dynamic and RAID disks in Windows

Endpoint Encryption works at sector level, consequently it does not support software-based dynamic disks and software based RAID.

Hardware RAID – Endpoint Encryption is untested in this mode, but may work properly in a situation where pure Hardware RAID has been implemented. However, Endpoint Encryption can't support diagnostic or disaster recovery in this situation.

HP Notebooks with SATA hard disks

McAfee and HP discovered an issue with the BIOS support for SATA hard disks on HP Notebooks, which makes writing to the hard disk in SATA Native mode unreliable. The issues has been confirmed on the HP Compaq nw8440 Mobile Workstation, HP Compaq nc8430 Notebook PC, and HP Compaq nx8420 Notebook PC.

If SATA Native Mode is enabled on these systems, the following issues eventually occur due to incorrect writing of data by the HP BIOS:

- Corrupt graphics and text in Pre-boot, missing users, missing tokens.
- Data Store Corrupt errors.
- Missing Attribute errors.
- **Unknown User** where the user previously functioned and has not been removed.

This issue is present in BIOS versions prior to F.10, released 17th April 2007. In these releases to prevent this issue occurring, please disable SATA Native Mode in your notebooks BIOS. You can obtain BIOS version F.10 and greater through your HP support service. If you are using a BIOS version of F.10 or greater, then this issue is not relevant. Download the drivers and software available from:
http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?prodNameId=1839208&lang=en&cc=us&taskId=135&prodClassId=-1&prodTypeId=321957&prodSeriesId=18391.

General Notes

- Users upgrading from EEPC 6.x should be aware that a new default theme is shipped as part of the 7.0.x releases. If you are using customized themes with EEPC 6.x, then recreate your custom themes from the EEPC 7.0 Patch 3 default theme after the upgrade. This will make sure that the correct user interface is displayed and the correct audio is heard. Failure to do so will continue to display the EEPC 6.x user interface and use the EEPC 6.x audio. Those users who wish to deploy the new default theme to all their existing endpoints or have their own custom theme should follow these steps to make sure they are using the correct theme during PBA.

  1. Create a Theme Deployment task and assign it to all of your endpoints.
  2. Make sure that you have the desired theme selected in the Theme section of the Product Policy, that is, McAfee Default or your own custom theme based on the EEPC 7.x default theme.
  3. After upgrading an endpoint, allow the Theme Deployment and Policy Enforcement tasks to complete before restarting the system.

  Note The size limit of the PNG file that can be uploaded is 2.5 MB.

- If you are using Policy Assignment Rules to assign specific Endpoint Encryption User-Based Policies (UBP) to users, see the *McAfee Endpoint Encryption 7.0 Patch 1 Product Guide* to

learn how to configure these users to continue to use Policy Assignment Rules in EEPC 7.0 Patch 3. This must be done prior to deploying the Endpoint Encryption (EE) Agent/PC to the clients. Failing to configure users correctly will result in users returning to the default User Based Policy assigned at system level.

- If you are using the autoboot feature in EEPC 5.x.x, please be advised that at least one EEPC user must be assigned to each client system to be upgraded to EEPC 7.0 Patch 3 successfully.

Note In EEPC 6.x.x/7.x.x, the autoboot feature no longer requires the use $autoboot$, therefore do not create this use as a valid user in Active Directory. In the context of the bullet above, one EEPC user refers to a valid Active Directory user.

- On upgrading from EEPC 6.x and EEPC 7.0.x to EEPC 7.0 Patch 3, the EEPC MBR is backed up to the McAfee ePO server. To avoid overloading the server, we recommend that you roll out the upgrade in batches of around 5000 systems.
- Out-of-band user management does not work when the action is performed on the client system at PBA through CIRA.
- RemoveEE is not supported in the UEFI version of the standalone EETech for Opal. The users should use the WinPE version of EETech if they wish to remove EE on a UEFI system. The reason for this is that the Opal removal process is highly complex on a UEFI system and is technically challenging to put in a standalone version of EETech.
- The built in track pad/mouse pad/touch interface may not work in Pre-Boot on UEFI booting systems. The reason for this is that OEM might not bundle a suitable UEFI driver for the device in the firmware. The track pad/mouse pad requires the UEFI Simple Pointer Protocol and the touch interface requires the Absolute Pointer Protocol to work correctly.
- With HIPS 7.0 Patch 1, HIPS Security content 8.0.0.4611 is required for successful EEPC installation on the client. EEPC installation will fail if this security content is not updated on the client.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version 3 Select a product document
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

Copyright © 2014 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.